Notes from 2003 Software Developers Conference Encryption Breakout Session

- On June 6, 2003, as part of the ETA Software Developers Conference at the Hyatt Regency Hotel, in Crystal City, VA, Electronic Tax Administration (ETA) in conjunction with Modernization and Information Technology Services (MITS) co-hosted a breakout session to discuss encryption alternatives that IRS is exploring. Approximately seventeen external partners from fifteen companies attended. In addition, IRS contractors and IRS employees working on the encryption initiative were also present. Beatrice Howell and Ron Rosh, IRS, greeted everyone and explained that the purpose of the session was to hear from the external Software Developers regarding preferences and opinions on the file encryption alternatives that the IRS is considering. Beatrice Howell introduced the idea of a user council be created, comprised of IRS and volunteers from the developer community. At the end of the session, some volunteers signed up. Paul Masucci, IRS, introduced each alternative and opened the floor for feedback.

- **Feedback Regarding the three encryption alternatives presented were**:

    - File Encryption
        - Can be inserted and extracted easily.
        - PGP and GPG protocols are easy to drop in and are already being used by some software developers for other projects.
        - Does not require any TeleCom involvement.
        - Can use same software, same equipment, and would have to make little changes to their scripts.
        - Platform and Operating System neutral.
        - It will not interfere with other solutions being developed.
        - Concern is the "last link" and location of decryption process.
        - Key management is significant.
        - Key management needs to be researched, but everyone wanted it to follow the KISS principle.
        - Private key should be linked to Transmitter.
        - Suggested having one IRS public key.
        - Suggested having one public key for all software packages instead of one for each package; otherwise the question of how key would be handled if software is re-sold.
        - Imbedding the key is preferable to a menu choice in the Trading Partner Interface.

    - Virtual Private Network (VPN)
        - Extremely problematic.
        - Third Party software required.

        - Expensive.
        - COTS limitations.
        - Network and/or platform constraints.
        - Requires more support from Software Developers for end-user training and use problems.
        - Software Developers do not "touch" each end user, so installing end-user client software is extremely difficult.

    - Secure Socket Layer (SSL) with Modem
        - Requires embedded software on the client.
        - Scripting would be difficult when there is no dial tone.
        - Switching protocols over TelNet would be difficult.
        - Layering, and debugging issues.
        - Platform dependencies.
        - Pop-ups would be a problem.
        - Requires complex interface.
        - Requires more interactions
        - Support would be more expensive.
        - None of the states use this.

    - Secure Socket Layer (SSL) over the Internet
        - Preference expressed for "Internet SSL" versus non-Internet SSL.
        - More simple than with modem.
        - Support is cheaper because of networking.
        - Some already receive returns from their clients this way.
        - Industry standard.
        - Some customers do not have Internet Service Provider.

- **Additional notes for the encryption alternatives**:
    - VPN was almost unanimously not preferred because of end user interaction and impact.
    - File encryption and SSL over the Internet should be explored; both could be offered as solutions.
    - Dedicated filers could still use encryption on their routers instead of one of the above solutions.
    - Selected encryption solution should include compression functions.
    - January 2004 date for their receipt of the Interface Control Document is acceptable.
    - Implementation for November 2004 assurance testing cycle is acceptable.

- **Order of preference** (most to least preferred, as expressed by session attendees)
    - File encryption (with minimal key management issues)
    - Internet SSL

- Modem SSL
- VPN

For questions or comments about these notes, you may contact Robert L. Clark, 202-283-5488 (Robert.l.clark@irs.gov) or Carolyn E. Davis, 202-283-0589 (Carolyn.e.davis@irs.gov).